UNIVERSITY OF TORONTO
3 1761 00469307 3

61
47

135232
19/11/14

SUR LA

DIVISIBILITÉ DES POLYNOMES ENTIERS

A PLUSIEURS VARIABLES

PAR

M. Ch. MÉRAY

PARIS,
GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE
DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.

1907

QH
161
.M47

SUR LA DIVISIBILITÉ DES POLYNOMES ENTIERS A PLUSIEURS VARIABLES;

PAR M. CH. MÉRAY.

1. Ayant été ramené à cette théorie, il y a une vingtaine d'années, par le besoin accidentel de l'un de ses points [le théorème du n° 10, III (*inf.*)], je ne l'ai vue nulle part traitée d'une manière tout à fait satisfaisante, et j'ai aperçu le principe de l'exposition que j'en vais présenter.

On saisira facilement l'esprit général de la méthode en remarquant à chaque pas, *qu'elle consiste dans la combinaison des procédés propres au cas d'une seule variable, opérée par voie de récurrence, c'est-à-dire par la réduction d'un cas quelconque à un autre où le degré d'une variable au moins s'est abaissé dans l'un au moins des polynomes à manier, sans s'élever dans les autres.*

Je représenterai par

$$(1) \qquad s,\ t,\ \ldots,\ v,\ x,\ y,\ \ldots,\ w$$

les variables indépendantes qui, en nombre fixe h, seront exclusivement engagées, en totalité ou en partie seulement, dans les polynomes dont je parlerai, et je commence par rappeler et préciser certains faits préliminaires.

I. Un *monome* (entier) en (1) est une expression formée en prenant quelque produit de puissances de

ces variables, à exposants entiers, positifs ou nuls,

$$s^{\sigma} t^{\tau} \ldots v^{\varphi} x^{\xi} y^{\eta} \ldots w^{\psi},$$

puis celui

$$c\, s^{\sigma} t^{\tau} \ldots v^{\varphi} x^{\xi} y^{\eta} \ldots w^{\psi}$$

du précédent, par quelque *coefficient* constant c.

On *ordonne* ce monome *par rapport à* un groupe donné de ses variables,

$$(2) \qquad x, \quad y, \quad \ldots, \quad w,$$

dites alors *ordonnatrices,* en l'écrivant

$$(c\, s^{\sigma} t^{\tau} \ldots v^{\varphi})\, x^{\xi} y^{\eta} \ldots w^{\psi},$$

c'est-à-dire en le considérant comme formé par la multiplication de ses facteurs en (2) seulement et du produit de son coefficient par ceux en

$$(3) \qquad s, \quad t, \quad \ldots, \quad v$$

seulement, produit qui, à ce point de vue, lui constitue un *nouveau coefficient* ne dépendant plus des variables ordonnatrices.

Par rapport aux variables (2), deux monomes sont *semblables* si, dans l'un et dans l'autre, elles portent des exposants respectivement égaux. Autrement, ils sont *dissemblables.*

Quand le groupe (2) comprend la totalité (1) des variables de la question, la relativité de cette similitude n'est pas mentionnée.

II. Un *polynome* (entier) en (1) se forme en prenant un seul monome à la rigueur, ou, habituellement, la somme de plusieurs dissemblables deux à deux (I), qui soit ses *termes,* et dont les coefficients gardent ce nom pour cette nouvelle expression.

On *ordonne* un polynome *par rapport* aux variables d'un groupe tel que (2), en ordonnant ainsi ses divers termes (1); en sommant, avec chacun d'eux, tous ceux qui lui sont semblables relativement au même groupe, puis en faisant l'addition de toutes ces sommes. On obtient ainsi un polynome en (2), ayant pour *nouveaux coefficients* des polynomes en (3), et, dans leur ensemble, les coefficients proprement dits de ces derniers polynomes se confondent avec ceux mêmes du proposé.

III. *Par rapport* à un groupe de variables tel que (2), le *degré apparent* d'un polynome est le nombre obtenu en formant, pour chaque terme, la somme des exposants portés par ces variables seulement, et prenant la plus grande valeur de ces diverses sommes.

Son *degré effectif* est le résultat de la même opération exécutée sur ceux seulement de ses termes dont les coefficients sont $\neq 0$. C'est lui que désigne toujours le mot *degré* employé seul, sauf mention qu'il s'agit de l'autre.

Quand le degré (effectif) est nul, le polynome, sans cesser de dépendre nominalement des variables (2), n'en dépend pas en réalité; car, affectées des exposants 0, 0, ..., 0 dans les termes à coefficients $\neq 0$, ces variables n'y introduisent que les facteurs constants 1, 1, ..., 1, et les autres termes ont la valeur constante 0, quelles que soient celles des leurs. Nous dirons alors que le polynome est *déchevêtré* des variables (2) en question.

Il en est *enchevêtré* si chacune d'elles porte un exposant > 0 dans quelque terme pourvu d'un coefficient $\neq 0$.

Dans ces diverses dénominations, la mention de

relativité s'omet habituellement, quand le groupe considéré embrasse la totalité (1) des variables de la question.

IV. *Un polynome est identiquement nul, ou non, selon que ses coefficients sont, numériquement, tous nuls, ou non.*

Si tous les coefficients sont nuls, il est évident que le polynome n'a jamais que la valeur 0.

Sinon, soient un polynome enchevêtré de la seule variable x (III) et $c_\mu x^\mu$ son terme de moindre degré μ parmi ceux dont les coefficients sont $\neq 0$. La valeur du polynome pouvant s'écrire $(c_\mu + \varepsilon) x^\mu$, où celle de ε peut devenir aussi petite qu'on le veut, moyennant l'attribution à x d'une valeur suffisamment petite *quoique non nulle,* on peut ainsi rendre ε numériquement $< c_\mu$, rendre non nulles en conséquence les valeurs des deux facteurs et cette expression, simultanément, celle par suite de leur produit, c'est-à-dire de l'expression elle-même. Le polynome considéré n'est donc pas nul identiquement.

S'il s'agit d'un polynome enchevêtré de deux variables x, y seulement, soit $c_{\mu,\nu} x^\mu y^\nu$ un de ses termes à coefficient $\neq 0$, et $(\ldots + c_{\mu,\nu} x^\mu + \ldots) y^\nu$ son terme en y^ν dans le résultat de son ordination par rapport à y (II). D'après ce qui vient d'être constaté, et, comme le polynome en x seulement, $\ldots + c_{\mu,\nu} x^\mu + \ldots$, n'est pas nul identiquement, parce que le coefficient $c_{\mu,\nu}$ de son terme laissé en évidence ne l'est pas numériquement, on peut assigner à x une valeur x' qui rend la sienne, $\mathcal{C}'_\nu$, $\neq 0$. Pour $x = x'$, le polynome proposé se particularise en $\ldots + \mathcal{C}'_\nu y^\nu + \ldots$, polynome en y seulement dont le terme mis en évidence a un coefficient $\neq 0$, auquel, en conséquence, et par

une nouvelle application de ce qui précède, on peut faire prendre quelque valeur $\neq 0$. Le proposé n'est donc pas nul identiquement.

De là, on passe semblablement aux polynomes enchevêtrés de 3 variables, puis de 4, 5, ..., etc.

Pour abréger, nous dirons un polynome *nul* ou *non-nul,* selon que ses coefficients seront tous nuls, ou non. Sauf mention du contraire, un polynome est toujours sous-entendu non-nul, et, le plus souvent, émondé de ses termes nuls (qui sont sans influence sur sa valeur numérique).

V. *Le produit de plusieurs polynomes est nul* (IV) *quand l'un au moins des facteurs est tel, mais non-nul quand aucun d'eux n'est nul.*

Le premier point résulte immédiatement de ce que, dans ce produit, le coefficient de tout terme est une somme de parties dont chacune se forme en multipliant entre eux les coefficients de termes des polynomes facteurs, pris respectivement dans tous ceux-ci.

D'où la nullité de chacune de ces parties, contenant ainsi un ou plusieurs facteurs nuls numériquement, puis celle de leur somme, coefficient considéré du polynome produit, puis celle de ce polynome.

Pour le second point, considérons d'abord le cas de deux facteurs enchevêtrés de la seule variable x, et soient μ', μ'' leurs degrés (effectifs) (III), $c'_{\mu'}x^{\mu'}$, $c''_{\mu''}x^{\mu''}$ leurs termes de ces degrés. Il est visible que le produit (amené à la forme normale) contient le terme $c'_{\mu'}c''_{\mu''}x^{\mu'+\mu''}$ dont le coefficient n'est pas nul, puisque ses facteurs, $c'_{\mu'}$, $c''_{\mu''}$, ne le sont ni l'un ni l'autre. Le polynome produit est donc non-nul.

De là, aux cas de deux facteurs enchevêtrés de 2 variables, puis de 3, 4, ..., on passe par voie d'ordina-

tions variées et de récurrence, comme nous venons de le faire dans une circonstance analogue (IV).

Soit enfin $\mathfrak{P}'\mathfrak{P}''\ldots\mathfrak{P}^{(j)}$ un produit de j polynomes non nuls quelconques. En vertu de ce qui précède, sont non nuls : les produits $\mathfrak{P}'\mathfrak{P}''$, puis

$$(\mathfrak{P}'\mathfrak{P}'')\mathfrak{P}''' = \mathfrak{P}'\mathfrak{P}''\mathfrak{P}''',$$

puis ..., puis enfin $(\mathfrak{P}'\mathfrak{P}''\ldots)\mathfrak{P}^{(j)}$ qui est le produit en question.

VI. *Par rapport à tout groupe des variables* (I), *le degré* (*effectif*) (III) *d'un produit de plusieurs polynomes est égal à la somme de ceux de ses facteurs.*

Dans un premier polynome, soit μ' son degré de ce genre, $(\mathcal{G}')_{\mu'}$ le groupe formé par tous ses termes (non nuls) de même degré μ', et $(\mathcal{G}')_{\nu'}$, $(\mathcal{G}')_{\varpi'}$, ... les groupes analogues, de degrés $\nu' < \mu'$, $\varpi' < \nu'$, ..., en sorte que la forme

$$(\mathcal{G}')_{\mu'} + (\mathcal{G}')_{\nu'} + (\mathcal{G}')_{\varpi'} + \ldots$$

puisse être donnée à ce polynome. Soit encore

$$(\mathcal{G}'')_{\mu''} + (\mathcal{G}'')_{\nu''} + (\mathcal{G}'')_{\varpi''} + \ldots$$

la forme analogue donnée à un autre polynome dont le degré est μ''. Le produit de tous deux peut être écrit

$$(\mathcal{G}')_{\mu'}(\mathcal{G}''')_{\mu''} + \ldots,$$

et, en premier lieu, le produit partiel laissé en évidence est non-nul puisque chacun de ses deux facteurs est tel (IV); en second lieu, son développement ne contient évidemment que des termes élémentaires de degré commun $\mu' + \mu''$; en troisième lieu, celui des produits partiels non écrits ne peut donner que des

termes de degrés $< \mu' + \mu''$. On en conclut que le degré du produit des deux polynomes considérés est bien égal à $\mu' + \mu''$, somme de ceux des facteurs.

De ce cas, de deux facteurs seulement, on passe à ceux de 3, 4, ..., par le moyen employé à la fin de l'alinéa précédent (V).

VII. *Deux polynomes sont identiquement égaux ou non selon que, respectivement, les termes (non nuls) de chacun sont semblables à ceux de l'autre et pourvus de coefficients numériquement égaux, ou bien qu'il n'en est pas ainsi.* Car le polynome obtenu en prenant leur différence a pour coefficients les différences de ceux des termes semblables dans les proposés, et il est nul dans le premier cas, non-nul dans le second (IV).

Suivant l'une ou l'autre alternative, nous dirons ces polynomes *égaux* ou *inégaux*.

2. On *divise* un polynome donné $\mathfrak{M}$ *par* un autre $\mathfrak{N}$, on fait la *division* du premier par le second, en en cherchant un troisième dont le produit par le second soit égal au premier (1, VII).

Dans cette opération, $\mathfrak{M}$, $\mathfrak{N}$ prennent les noms de *dividende, diviseur,* et, si l'on peut lui trouver quelque résultat $\mathfrak{Q}$, on exprime cette possibilité en disant que $\mathfrak{M}$ est *divisible par* $\mathfrak{N}$, que $\mathfrak{Q}$ est le *quotient* de la division.

Les moyens d'exécution dérivent des observations résumées ci-après.

I. *Si le diviseur est nul* (1, IV), et, comme, en conséquence, son produit par un polynome quelconque l'est toujours (*Ib.*, V), *la division est impossible quand le dividende ne l'est pas, possible quand il*

l'est aussi, mais alors avec indétermination du quotient.

II. *Quand le diviseur est non-nul, le quotient de toute division possible est unique.* Si, en divisant $\mathfrak{M}$ par $\mathfrak{N}$, on trouvait deux quotients inégaux $\mathfrak{Q}_1$, $\mathfrak{Q}_2$, la soustraction membre à membre des identités de définitions

$$\mathfrak{M} = \mathfrak{N}\mathfrak{Q}_1, \qquad \mathfrak{M} = \mathfrak{N}\mathfrak{Q}_2$$

conduirait à

$$0 = \mathfrak{N}(\mathfrak{Q}_1 - \mathfrak{Q}_2),$$

chose impossible, puisque dans ce produit de deux facteurs le second est non-nul, le premier supposé tel (*Ibid.*).

III. *Quand le dividende est nul, non le diviseur, la division est possible et le quotient est toujours nul.* Car l'identité à réaliser $0 = \mathfrak{N}\mathfrak{Q}$, sous la condition $\mathfrak{N} \neq 0$, l'est toujours et seulement par $\mathfrak{Q} = 0$ (*Ib.*).

Désormais, nous supposerons non nuls, le diviseur toujours, et aussi le dividende quand le contraire n'aura pas été spécifié.

IV. *Pour que la division soit possible, il est nécessaire que, par rapport à tout groupe des variables* (1), *le degré* (*effectif*) ω' *du dividende soit au moins égal à* ω'' *degré du diviseur; et, s'il en est ainsi, le degré analogue* ω *du quotient est donné* a priori *par la formule*

$$\omega = \omega' - \omega''. \tag{4}$$

S'il existe quelque quotient $\mathfrak{Q}$, dont le degré analogue soit ω, l'identité fondamentale $\mathfrak{M} = \mathfrak{N}\mathfrak{Q}$ entraîne $\omega' = \omega'' + \omega$ (1, VI), d'où $\omega' \geqq \omega''$ et (4).

Maintenant, nous pouvons passer à l'examen de trois cas simples, d'où se déduit la solution complète du problème.

Auparavant, il faut noter que, pour un groupe formé d'une seule variable u enchevêtrant le dividende, le diviseur et le quotient aux degrés υ', υ'', υ, on a aussi bien

$$\upsilon = \upsilon' - \upsilon'',$$

cas particulier de (4) dont l'emploi est continuel.

V. *Le dividende et le diviseur sont des formes*

$$(\mathfrak{M} =)\, \mathrm{M}(s, t, \ldots, v)\, x^{\xi'} y^{\eta'} \ldots w^{\psi'},$$
$$(\mathfrak{N} =)\, \mathrm{N}(s, t, \ldots, v)\, x^{\xi''} y^{\eta''} \ldots w^{\psi''},$$

monomes en x, y, ..., w, ayant pour coefficients des polynomes déchevêtrés de ces variables.

Si un quotient existe, son ordination par rapport au même groupe (2) ne peut donner qu'un terme, car, autrement, son produit par $\mathfrak{N}$, ordonné de la même manière, en contiendrait plus d'un aussi, alors que $\mathfrak{M}$ n'en a qu'un seul. Il est donc de la même forme

$$(\mathfrak{Q} =)\, \mathrm{Q}(s, t, \ldots, v)\, x^{\xi} y^{\eta} \ldots w^{\psi},$$

où $\mathrm{Q}(s, t, \ldots, v)$, ξ, η, ..., ψ sont : un polynome déchevêtré de x, y, ..., w, des exposants entiers non négatifs, à choisir de manière à donner identiquement

$$\begin{aligned} &\mathrm{M}(s, t, \ldots, v)\, x^{\xi'} y^{\eta'} \ldots w^{\psi'} (= \mathfrak{M} = \mathfrak{N}\mathfrak{Q}) \\ &\quad = [\mathrm{N}(s, t, \ldots, v)\, \mathrm{Q}(s, t, \ldots, v)]\, x^{\xi''+\xi} y^{\eta''+\eta} \ldots w^{\psi''+\psi}. \end{aligned}$$

A cette fin, les conditions nécessaires et suffisantes sont visiblement :

1° Pour que le premier membre soit semblable au dernier, relativement à x, y, ..., w, que l'on ait

$$\xi' = \xi'' + \xi,\ \eta' = \eta'' + \eta,\ \ldots,\ \psi' = \psi'' + \psi,$$

d'où

$$\xi = \xi' - \xi'', \eta = \eta' - \eta'', \ldots, \psi = \psi' - \psi'' \quad (Cf. \text{IV});$$

2° Pour que les coefficients des termes semblables dans leurs développements complets soient respectivement égaux, que l'on ait identiquement

$$M(s, t, \ldots, v) = N(s, t, \ldots, v)\, Q(s, t, \ldots, v),$$

c'est-à-dire que M soit divisible par N et que Q soit pris égal au quotient de cette division.

Si donc il y a possibilité, on aura

$$\mathfrak{Q}(= \mathfrak{M} : \mathfrak{N}) = (M : N)\, x^{\xi'-\xi''} y^{\eta'-\eta''} \ldots w^{\psi'-\psi''},$$

ce qui ramène le problème au cas de deux polynomes, M, N, *impliquant des variables en nombre inférieur à celui des primitives* (1).

VI. *Le dividende* $\mathfrak{M}$ *est quelconque, le diviseur* $\mathfrak{N}$ *est déchevêtré des variables* (2).

La possibilité de la division exige, comme condition nécessaire et suffisante, *que les coefficients* M_1, M_2, ... *du dividende ordonné par rapport à ce groupe soient tous divisibles par* $\mathfrak{N}$. *Et, sous cette condition, ceux du quotient pareillement ordonné sont les quotients* $M_1 : \mathfrak{N}$, $M_2 : \mathfrak{N}$, ... C'est ce que montre bien facilement l'identification de $\mathfrak{M}$ au produit de $\mathfrak{N}$ par un quotient hypothétique $\mathfrak{Q}$ ordonné de la même manière (*Cf.* V). *L'opération est ramenée au cas de polynomes dépendant des variables* (3) *seulement.*

La condition formulée entraîne visiblement la divisibilité par $\mathfrak{N}$ *des coefficients de* $\mathfrak{M}$, *ordonné par rapport à tout sous-groupe des variables* (2).

VII. *Le dividende et le diviseur sont enchevêtrés d'une même variable* x, *aux degrés* $\mathfrak{m}$, $\mathfrak{n}$ [$\leqq \mathfrak{m}$ (IV)].

Soient alors

$$(\mathfrak{M} =) \, M_{m} x^{m} + M_{m-1} x^{m-1} + \ldots,$$
$$(\mathfrak{N} =) \, N_{n} x^{n} + N_{n-1} x^{n-1} + \ldots,$$

les résultats de leur ordination par rapport à x suivant ses puissances décroissantes, les M, N étant des polynomes déchevêtrés de cette variable. On pourra commencer et poursuivre la « division algébrique » du premier par le second, comme si les M, N n'étaient que des constantes, cela aussi longtemps que les degrés en x, des premiers termes du dividende et des dividendes partiels consécutifs, resteront $\geqq n$ et leurs premiers coefficients divisibles par N_n.

Quand ces divisibilités se trouvent exister jusqu'au bout et qu'on arrive à un reste nul, on constatera bien facilement que la division de $\mathfrak{M}$ par $\mathfrak{N}$ est possible et que le quotient ordonné par rapport à x se forme terme à terme, comme si cette variable était la seule de la question.

Quand il n'en est pas ainsi, on reconnaîtra avec la même facilité que $\mathfrak{M}$ n'est pas divisible par $\mathfrak{N}$.

Ceci ramène le problème à un cas précédent (V) *et à celui de polynomes dépendant de $h - 1$ variables seulement, par la technique propre au cas élémentaire où le dividende et le diviseur ne sont enchevêtrés que d'une seule variable.*

VIII. Comme chacun de ces moyens déchevêtre toujours de quelque variable, l'un au moins des polynomes qu'il laisse à manier, et cela sans enchevêtrer les autres, il est clair que *leur enchaînement en récurrences convenables conduira sûrement à la réponse comportée par la division proposée.*

IX. On aperçoit immédiatement, que *tout polynome*

est divisible, tant par lui-même, que par une constante quelconque ($\neq 0$). Dans le premier cas, le quotient est 1; dans le second, on l'obtient en divisant simplement les coefficients du dividende par la constante diviseur (VI).

3. A la notion de divisibilité, les suivantes se rattachent très étroitement.

I. Deux polynomes sont *semblables* quand l'un est divisible par l'autre et que le quotient de leur division se réduit à une constante, relation évidemment réciproque. Ils sont *dissemblables* s'il en est autrement.

II. Les *diviseurs* d'un polynome donné sont ceux de degrés > 0 qui le *divisent,* c'est-à-dire par lesquels il est divisible (2). *Parmi eux, se trouvent toujours lui-même* (*Ib.* IX) *et, visiblement, les polynomes semblables à tout diviseur qu'on lui connaîtrait déjà.*

On notera que *les constantes ne comptent pas comme diviseurs,* bien qu'elles divisent tous les polynomes quand elles sont $\neq 0$ (*Ibid.*).

Un polynome est *premier,* quand, étant de degré $\neq 0$, il n'a d'autres diviseurs que ses semblables (I) (lui-même compris). *Tel est, visiblement, un polynome quelconque du premier degré.*

III. *Tout polynome non premier peut être mis sous forme d'un produit de facteurs premiers* (*dissemblables ou semblables*)*; et le nombre de ces facteurs est limité,* puisque leurs degrés, tous > 0, ont celui de proposé pour somme. Ce polynome est dit *composé* (de tels facteurs).

(*Dans le cas tout spécial d'un polynome à une*

seule variable, de degré ω, *ces facteurs premiers sont de degré commun* $= 1$, *et en nombre* $= \omega$. Ceci résulte du point fondamental de la théorie des équations entières à une inconnue.)

IV. Un diviseur est *commun* à plusieurs polynomes, quand il divise chacun d'eux séparément.

Quand des polynomes ont un diviseur commun, celui-ci divise aussi toute combinaison faite d'eux par des additions et soustractions; le quotient est la combinaison homonyme de ceux de leurs divisions par ce diviseur.

Des polynomes sont *premiers entre eux,* quand ils sont dépourvus de tout diviseur commun. Ils ne sont alors divisibles simultanément, que par des constantes $\neq 0$.

Des polynomes dissemblables et premiers chacun (dans le sens absolu du mot) sont toujours premiers entre eux.

V. Les *multiples* d'un polynome donné sont tous ceux que celui-ci divise; ils se confondent évidemment avec ses produits par tous les polynomes imaginables; en particulier, ils comprennent ses semblables.

Tout diviseur d'un polynome divise l'un quelconque de ses multiples; le quotient est le produit de celui de la division du polynome par le diviseur, et du multiplicateur qui a fourni le multiple considéré.

Les *multiples communs* de plusieurs polynomes sont tous ceux que divise chacun des proposés.

4. La *division algébrique* est susceptible d'une extension dont nous allons avoir besoin.

Les polynomes $\mathfrak{M}$, $\mathfrak{N}$ du n° 2, VII *étant repris, on peut en assigner un troisième* ${}^{(x)}\mathfrak{P}$ *déchevêtré de* x, *qui rende possible la* division algébrique *du produit* ${}^{(x)}\mathfrak{P}\mathfrak{M}$ *par* $\mathfrak{N}$, *c'est-à-dire qui permette la formation de l'identité.*

$$(5) \qquad {}^{(x)}\mathfrak{p}\mathfrak{M} = \mathfrak{Q}\mathfrak{N} + \mathfrak{R},$$

où $\mathfrak{Q}$ *et* $\mathfrak{R}$ *sont des polynomes dont les degrés en* x *ont des valeurs* $= \mathfrak{m} - \mathfrak{n}$ *et* $< \mathfrak{n}$.

I. Soient $N_{\mathfrak{n}} x^{\mathfrak{n}}$ toujours, le premier terme de $\mathfrak{N}$, puis $M^{(i)}_{\mathfrak{m}_i} x^{\mathfrak{m}_i}$ celui d'un dividende partiel $\mathfrak{M}^{(i)}$ ordonné comme $\mathfrak{M}$, $\mathfrak{N}$ l'ont été. Aussi longtemps que $\mathfrak{m}_i$ sera $\geqq \mathfrak{n}$, on assurera la possibilité de la division partielle correspondante en multipliant $\mathfrak{M}^{(i)}$ par quelque polynome ${}^{(x)}\mathfrak{p}^{(i)}$ déchevêtré de x, choisi de manière à donner avec $M^{(i)}_{\mathfrak{m}_i}$ un produit ${}^{(x)}\mathfrak{p}^{(i)} M^{(i)}_{\mathfrak{m}_i}$ qui soit divisible par $N_{\mathfrak{n}}$; à cette fin, il suffira de prendre, pour le multiplicateur ${}^{(x)}\mathfrak{p}^{(i)}$, $N_{\mathfrak{n}}$ toujours (3, V), un polynome de degré moindre parfois (16, *inf.*), 1 même seulement, quand la division partielle à exécuter sera possible d'emblée, c'est-à-dire quand $M^{(i)}_{\mathfrak{m}_i}$ se trouvera divisible par $N_{\mathfrak{n}}$.

En représentant alors par $\mathfrak{q}^{(i)}$ le quotient

$$\left[\left({}^{(x)}\mathfrak{p}^{(i)} M^{(i)}_{\mathfrak{m}_i}\right) : N_{\mathfrak{n}}\right] x^{\mathfrak{m}_i - \mathfrak{n}},$$

par $\mathfrak{M}^{(i+1)}$ la différence ${}^{(x)}\mathfrak{p}^{(i)}\mathfrak{M}^{(i)} - \mathfrak{q}^{(i)}\mathfrak{N}$, dont le degré en x est $< \mathfrak{m}_i$, il vient

$$(6) \qquad {}^{(x)}\mathfrak{p}^{(i)}\mathfrak{M}^{(i)} = \mathfrak{q}^{(i)}\mathfrak{N} + \mathfrak{M}^{(i+1)}.$$

II. En faisant successivement ici $i = 0, 1, 2, \ldots$, on trouvera

$$(7) \qquad \left\{\begin{array}{l} {}^{(x)}\mathfrak{p}\mathfrak{M} \phantom{{}^{(1)}} = \mathfrak{q}\mathfrak{N} \phantom{{}^{(1)}} + \mathfrak{M}^{(1)}, \\ {}^{(x)}\mathfrak{p}^{(1)}\mathfrak{M}^{(1)} = \mathfrak{q}^{(1)}\mathfrak{N} + \mathfrak{M}^{(2)}, \\ {}^{(x)}\mathfrak{p}^{(2)}\mathfrak{M}^{(2)} = \mathfrak{q}^{(2)}\mathfrak{N} + \mathfrak{M}^{(3)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{array}\right.$$

et l'on poursuivra aussi longtenps que $\mathfrak{m}_{i+1}$ degré de $\mathfrak{M}^{(i+1)}$ restera $\geqq \mathfrak{n}$. Comme les entiers $\mathfrak{m}, \mathfrak{m}_1, \mathfrak{m}_2, \ldots$ vont sans cesse en diminuant de 1 au moins chaque fois, on atteindra certainement une différence $\mathfrak{M}^{(j+1)}$ dont le degré sera $< \mathfrak{n}$, à laquelle, en conséquence, on sera forcé de s'arrêter; et la récurrence (7) se terminera par

$$(8 \qquad \left\{ \begin{array}{l} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ {}^{(x)}\mathfrak{p}^{(j-1)}\,\mathfrak{M}^{(j-1)} = \mathfrak{q}^{(j-1)}\,\mathfrak{N} + \mathfrak{M}^{(j)}, \\ {}^{(x)}\mathfrak{p}^{(j)}\,\mathfrak{M}^{(j)} \qquad = \mathfrak{q}^{(j)}\,\mathfrak{N} \quad + \mathfrak{M}^{(j+1)}. \end{array} \right.$$

Pour obtenir enfin la relation cherchée (5), il suffit maintenant d'ajouter membre à membre celles de l'ensemble (7) et (8), multipliées respectivement par les produits

$$(9) \qquad \left\{ \begin{array}{llll} {}^{(x)}\mathfrak{p}^{(1)}\,{}^{(x)}\mathfrak{p}^{(2)}\,{}^{(x)}\ldots\mathfrak{p}^{(j)}\,1, & {}^{(x)}\mathfrak{p}^{(2)}\,{}^{(x)}\mathfrak{p}^{(3)}\ldots{}^{(x)}\mathfrak{p}^{(j)}\,1, & & \\ {}^{(x)}\mathfrak{p}^{(3)}\ldots{}^{(x)}\mathfrak{p}^{(j)}\,1, & \ldots, & {}^{(x)}\mathfrak{p}^{(j)}\,1, & 1, \end{array} \right.$$

puis de noter ${}^{(x)}\mathfrak{P}$, $\mathfrak{Q}$ et $\mathfrak{R}$ les sommes des produits de ces multiplicateurs par les ${}^{(x)}\mathfrak{p}, \ldots$, par les $\mathfrak{q}, \ldots$ et $\mathfrak{M}^{(j+1)}$.

Les multiplicateurs (9) étant, comme leurs facteurs ${}^{(x)}\mathfrak{p}, \ldots$, tous déchevêtrés de x, on observera : que ${}^{(x)}\mathfrak{P}$ est tel, que le degré de $\mathfrak{Q}$ en x est $\mathfrak{m} - \mathfrak{n}$ puisque ceux de $\mathfrak{q}, \mathfrak{q}^{(1)}, \mathfrak{q}^{(2)}, \ldots$ sont $\mathfrak{m} - \mathfrak{n}, \mathfrak{m}_1 - \mathfrak{n}, \mathfrak{m}_2 - \mathfrak{n}, \ldots$, en suite sans cesse décroissante, que celui de

$$\mathfrak{R}\,[= \mathfrak{M}^{(j+1)}]$$

est $< \mathfrak{n}$, ce que nous avons déjà vu.

III. Il est essentiel de noter que *la construction de la relation* (5) *comporte simplement l'algorithme de la* division algébrique *à une seule variable ordonnatrice, combiné avec le maniement de polynomes déchevêtrés de cette variable, c'est-à-dire en contenant une de moins que les proposés.* On supprimerait même toute difficulté dans ce maniement, en pre-

nant invariablement N_u pour chacun des multiplicateurs ${}^{(x)}\mathfrak{p}$, ${}^{(x)}\mathfrak{p}^{(1)}$, ...

On pourrait donner à cette opération le nom de *quasi-division* relative à la variable ordinatrice x, de $\mathfrak{M}$ par $\mathfrak{N}$, à ces polynomes et à $\mathfrak{Q}$, $\mathfrak{R}$, ceux de *quasi-dividende, quasi-diviseur et quasi-quotient, quasi-reste*, à ${}^{(x)}\mathfrak{P}$ celui de *préparateur*.

La *division algébrique* n'étant que le cas particulier qui se présente quand le préparateur se réduit à 1, ces dénominations lui seraient bien mieux appropriées que celles du langage courant, puisque la *divisibilité* proprement dite du dividende par le diviseur n'est qu'une éventualité tout à fait exceptionnelle.

Au n° 16 (*inf.*), nous verrons qu'on peut toujours s'arranger de manière à rendre premiers entre eux le préparateur et le quasi-quotient.

5. *Les mêmes polynomes* $\mathfrak{M}$, $\mathfrak{N}$ (2, VII), (4) *étant encore repris, on peut en assigner trois autres,*

$$(9\,bis) \qquad \mathfrak{P},\quad \mathfrak{Q},\quad {}^{(x)}\mathfrak{F},$$

dont le dernier est déchevêtré de x, dont les deux premiers sont non-nuls (1, IV), *avec des degrés* $\mathfrak{p}$, $\mathfrak{q}$ *en x remplissant les conditions*

$$\mathfrak{p} < \mathfrak{n}, \quad \mathfrak{q} < \mathfrak{m},$$

et qui, tous trois, donnent avec $\mathfrak{M}$, $\mathfrak{N}$ *la relation*

$$(10) \qquad \mathfrak{P}\mathfrak{M} + \mathfrak{Q}\mathfrak{N} = {}^{(x)}\mathfrak{F}.$$

I. La suite de polynomes

$$\mathfrak{M},\ \mathfrak{N},\ \mathfrak{N}_1,\ \ldots,\ \mathfrak{N}_{i-1},\ \mathfrak{N}_i,\ \mathfrak{N}_{i+1},\ \mathfrak{N}_{i+2},\ \ldots,\ \mathfrak{N}_{j-1},\ \mathfrak{N}_j,\ \mathfrak{N}_{j+1},\ \mathfrak{N}_{j+2},$$

qui commence par les proposés et se poursuit par ceux qu'on rencontre successivement à partir du troisième, en prenant chaque fois le quasi-reste de la quasi-divi-

sion de l'antiprécédent par le précédent (4, III), s'arrête forcément à un terme $\mathfrak{N}_{j+2}$ déchevêtré de x. Leurs degrés en x forment effectivement une suite décroissante

$$(11) \qquad \mathfrak{m} \geqq \mathfrak{n} > \mathfrak{n}_1 > \mathfrak{n}_2 > \ldots > \mathfrak{n}_{j+1} > \mathfrak{n}_{j+2} (= 0),$$

puisque, dans toute quasi-division, celui du quasi-reste est inférieur à celui du quasi-diviseur; et un entier non négatif décroissant finit toujours par atteindre la valeur 0.

Si ces quasi-divisions ont

$$(12) \qquad {}^{(x)}\mathfrak{p}, \quad {}^{(x)}\mathfrak{p}_1, \quad \ldots, \quad {}^{(x)}\mathfrak{p}_i, \quad {}^{(x)}\mathfrak{p}_{i+1}, \quad \ldots, \quad {}^{(x)}\mathfrak{p}_j, \quad {}^{(x)}\mathfrak{p}_{j+1},$$

$$(13) \qquad \mathfrak{q}, \quad \mathfrak{q}_1, \quad \ldots, \quad \mathfrak{q}_i, \quad \mathfrak{q}_{i+1}, \quad \ldots, \quad \mathfrak{q}_j, \quad \mathfrak{q}_{j+1}$$

pour préparateurs et quasi-quotients, ceux-ci changés de signes, elles seront formulées par les relations,

$$(14) \qquad \left\{ \begin{array}{ll} {}^{(x)}\mathfrak{p}\,\mathfrak{M} + \mathfrak{q}\,\mathfrak{N} & = \mathfrak{N}_1, \\ {}^{(x)}\mathfrak{p}_1\,\mathfrak{N} + \mathfrak{q}_1\,\mathfrak{N}_1 & = \mathfrak{N}_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & , \\ {}^{(x)}\mathfrak{p}_i\,\mathfrak{N}_{i-1} + \mathfrak{q}_i\,\mathfrak{N}_i & = \mathfrak{N}_{i+1}, \\ {}^{(x)}\mathfrak{p}_{i+1}\,\mathfrak{N}_i + \mathfrak{q}_{i+1}\,\mathfrak{N}_{i+1} & = \mathfrak{N}_{i+2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ {}^{(x)}\mathfrak{p}_j\,\mathfrak{N}_{j-1} + \mathfrak{q}_j\,\mathfrak{N}_j & = \mathfrak{N}_{j+1}, \\ {}^{(x)}\mathfrak{p}_{j+1}\,\mathfrak{N}_j + \mathfrak{q}_{j+1}\,\mathfrak{N}_{j+1} & = \mathfrak{N}_{j+2}, \end{array} \right.$$

desquelles, en procédant de bas en haut, comme nous allons l'indiquer, on déduira successivement celles-ci en même nombre $j + 2$:

$$(15) \qquad \left\{ \begin{array}{ll} \mathrm{P}\,\mathfrak{M} + \mathrm{Q}\,\mathfrak{N} & = \mathfrak{N}_{j+2}, \\ \mathrm{P}_1\,\mathfrak{N} + \mathrm{Q}_1\,\mathfrak{N}_1 & = \mathfrak{N}_{j+2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & , \\ \mathrm{P}_i\,\mathfrak{N}_{i-1} + \mathrm{Q}_i\,\mathfrak{N}_i & = \mathfrak{N}_{j+2}, \\ \mathrm{P}_{i+1}\,\mathfrak{N}_i + \mathrm{Q}_{i+1}\,\mathfrak{N}_{i+1} & = \mathfrak{N}_{j+2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & , \\ \mathrm{P}_j\,\mathfrak{N}_{j-1} + \mathrm{Q}_j\,\mathfrak{N}_j & = \mathfrak{N}_{j+2}, \\ \mathrm{P}_{j+1}\,\mathfrak{N}_j + \mathrm{Q}_{j+1}\,\mathfrak{N}_{j+1} & = \mathfrak{N}_{j+2}. \end{array} \right.$$

Pour la dernière de (15), on prendra simplement celle de (14), c'est-à-dire qu'on fera

$$(16) \qquad P_{j+1} = {}^{(x)}\mathfrak{p}_{j+1}, \qquad Q_{j+1} = \mathfrak{q}_{j+1}.$$

Ensuite et généralement, on formera celle de (15) où l'indice commun de P, Q est i ($< j + 1$), en prenant le résultat de l'élimination de $\mathfrak{N}_{i+1}$ entre celle du même tableau où cet indice est $i + 1$, et celle de (14) où ${}^{(x)}\mathfrak{p}$, $\mathfrak{q}$ portent l'indice i, élimination faite de manière à donner

$$(17) \qquad P_i = {}^{(x)}\mathfrak{p}_i Q_{i+1}, \qquad Q_i = P_{i+1} + \mathfrak{q}_i Q_{i+1}.$$

Tout ceci ayant été exécuté, il suffira, pour former la relation cherchée (10), de prendre

$$(18) \qquad \mathfrak{P} = P, \qquad \mathfrak{Q} = Q, \qquad {}^{(x)}\mathfrak{F} = \mathfrak{N}_{j+2},$$

où $\mathfrak{N}_{j+2}$ est déchevêtré de x, et nous allons constater que P, Q remplissent les conditions imposées à $\mathfrak{P}$, $\mathfrak{Q}$ par l'énoncé.

II. Nous représenterons par ..., X_i, ... les degrés en x (effectifs) des polynomes (13) tous non-nuls comme quotients de quasi-divisions possibles à dividendes non-nuls, et par ..., Π_i, ..., par ..., X_i, ..., ceux des ..., P_i, ..., des Q_i, ..., dont nous allons reconnaître la non-nullité.

1° On a

$$\chi \geqq 0, \quad \chi_1 > 0, \quad \ldots, \quad \chi_i > 0, \quad \chi_{i+1} > 0, \quad \ldots, \quad \chi_j > 0, \quad \chi_{j+1} > 0.$$

Conséquence immédiate de l'égalité $\chi_i = \mathfrak{n}_{i-1} - \mathfrak{n}_i$ et des inégalités (11).

2° *Si les inégalités*

$$(19) \qquad P_{i+1} \neq 0, \qquad Q_{i+1} \neq 0,$$

$$(20) \qquad \Pi_{i+1} < X_{i+1}$$

existent, on aura encore

(21) $$P_i \neq 0, \qquad Q_i \neq 0,$$

avec

(22) $$\Pi_i = X_{i+1}, \qquad X_i = \chi_i + X_{i+1},$$

d'où, soit

(23) $$\Pi_i < X_i, \qquad si \quad i > 0 \qquad (1^\circ),$$

soit

(24) $\Pi \leqq X$, *si* $i = 0$, *selon que* $\chi = \mathfrak{m} - \mathfrak{n}$ *est* $\geqq 0$ (*Ib.*).

A cause de $Q_{i+1} \neq 0$ (19), de l'inégalité de principe ${}^{(x)}\mathfrak{p}_i \neq 0$, la première formule (17) donne immédiatement $P_i \neq 0$ (21), puis $\Pi_i = X_{i+1}$ (22), par sa combinaison avec le fait que les préparateurs (12) sont déchevêtrés de x.

Pour la même cause, et parce que $\mathfrak{q}_i \neq 0$, la dernière partie de l'expression de Q_i (17) est non-nulle, avec $\chi_i + X_{i+1}$ pour degré (en x); la première partie étant non nulle aussi (19), mais de degré Π_{i+1} qui est $< X_{i+1}$ (20), cette expression est non-nulle et de degré $\chi_i + X_{i+1}$. La seconde relation (19) conduit donc aux secondes relations (21) et (22), d'où (23) ou bien (24) suivant le cas.

3° A cause de (16) entraînant

$$\Pi_{j+1} = 0, \qquad X_{j+1} = \chi_{j+1} > 0,$$

les inégalités (19), (20) ont lieu pour $i = j + 1$; elles subsistent donc pour $i = j, j - 1, \ldots, 1, 0$ (2°).

4° En faisant $i = 1, 2, \ldots, j$ successivement dans la seconde égalité (22), se rappelant que $X_{j+1} = \chi_{j+1}$ (16) $= \mathfrak{n}_j - \mathfrak{n}_{j+1}$ parce que $\mathfrak{q}_{j+1}$ est le quasi-quotient

de la quasi-division de $\mathfrak{N}_j$ par $\mathfrak{N}_{j+1}$, et ajoutant membre à membre, il vient

$$(25)\quad \left\{\begin{aligned} X_1 &= \chi_1 + \chi_2 + \ldots + \chi_{j+1} \\ &= (\mathfrak{u} - \mathfrak{u}_1) + (\mathfrak{u}_1 - \mathfrak{u}_2) + \ldots + (\mathfrak{u}_j - \mathfrak{u}_{j+1}) \\ &= \mathfrak{u} - \mathfrak{u}_{j+1}. \end{aligned}\right.$$

On en conclut $\Pi = X_1$ (22) $< \mathfrak{u}$ (11).

Enfin, la seconde égalité (22) et (25) donnent immédiatement $X = (\mathfrak{m} - \mathfrak{u}) + (\mathfrak{u} - \mathfrak{u}_{j+1}) = \mathfrak{m} - \mathfrak{u}_{j+1}$, d'où $X < \mathfrak{m}$, dernier point nous restant à établir.

III. La formation de la relation (10) sous les conditions posées peut se nommer l'*élimination* de *x entre* les polynomes $\mathfrak{M}$, $\mathfrak{N}$; les polynomes (9 *bis*) en sont les *multiplicateurs* et le (polynome) *final*.

6. *Quand un polynome premier* $\mathfrak{N}$ (3, II) *divise le produit* $\mathfrak{L}\mathfrak{M}$ *de deux autres (premiers ou composés), mais non le second facteur* $\mathfrak{M}$, *il divise l'autre* $\mathfrak{L}$ *forcément.*

Notre démonstration comporte l'examen successif des cas distingués ci-après.

I. $\mathfrak{N}$ *n'est enchevêtré que de tout ou partie du groupe* (3); $\mathfrak{L}$, $\mathfrak{M}$ *le sont, tant de* (3) *que de* (2); *le théorème a été démontré dans tous les cas où chacun de ces trois polynomes ne l'est que de tout ou partie de* (3).

1° *Sous ces hypothèses, et si notre théorème est vrai quand* $\mathfrak{L}$, $\mathfrak{M}$, *enchevêtrés de* (3), *ne le sont en outre que de quelque sous-groupe de* (2), *il subsiste après l'adjonction d'une nouvelle variable x à ce sous-groupe.*

Cette adjonction ayant été faite, soient

$$(\mathfrak{L} =) \, L_l x^l + L_{l-1} x^{l-1} + \ldots,$$
$$(\mathfrak{M} =) \, M_m x^m + M_{m-1} x^{m-1} + \ldots$$

les résultats de l'ordination de ces polynomes par rapport à x, dont les coefficients L, M en sont déchevêtrés, et dont les termes ont été écrits dans l'ordre où leurs degrés (en x) décroissent.

Comme les M ne sont pas tous divisibles par $\mathfrak{N}$, sans quoi $\mathfrak{M}$ le serait (2, VI), contrairement à l'hypothèse, l'un d'eux au moins M_μ sera non divisible à l'exclusion de ses précédents M_m, M_{m-1}, ..., $M_{\mu-1}$, et en écrivant

$$\mathfrak{L}\mathfrak{M} - \mathfrak{L}(M_m x^m + M_{m-1} x^{m-1} + \ldots + M_{\mu-1} x^{\mu-1})$$
$$= \mathfrak{L}(M_\mu x^\mu + \ldots),$$

le second membre sera divisible par $\mathfrak{N}$ puisque les deux parties du premier le sont (3, IV), l'une par hypothèse, l'autre à cause de la même divisibilité des coefficients M_m, M_{m-1}, ..., $M_{\mu-1}$. Mais on a

$$\mathfrak{L}(M_\mu x^\mu + \ldots) = (L_l x^l + \ldots)(M_\mu x^\mu + \ldots)$$
$$= L_l M_\mu x^{l+\mu} + \ldots,$$

développement où le terme laissé en évidence n'en a visiblement aucun autre semblable. Il faut donc (2, VI) que $L_l M_\mu$, coefficient de ce terme, soit divisible par $\mathfrak{N}$, et, par suite, en vertu de l'hypothèse spéciale au présent sous-alinéa, que L_l le soit, puisque M_μ ne l'est pas.

On a ensuite

$$\mathfrak{L}(M_\mu x^\mu + \ldots) - L_l x^l (M_\mu x^\mu + \ldots)$$
$$= (L_{l-1} x^{l-1} + \ldots)(M_\mu x^\mu + \ldots),$$

produit encore divisible par $\mathfrak{N}$, comme les deux parties

du premier membre où L_l l'est. De même qu'à l'instant, et en vertu de la même hypothèse, la non divisibilité de M_μ entraînera la divisibilité de L_{l-1}, puis, successivement, de L_{l-2}, ..., L_0, puis finalement celle de $\mathfrak{L}$ (*Ib.*).

2° L'exactitude du point en question ayant été admise pour le cas où $\mathfrak{L}$, $\mathfrak{M}$ sont déchevêtrés de (2), ce qui précède l'étendra à ceux où l'on introduit dans ces polynomes les variables x d'abord, puis y après x, puis z après x et y, puis ..., puis w finalement.

II. *$\mathfrak{M}$ n'est enchevêtré que de tout ou partie de* (3); *$\mathfrak{L}$, $\mathfrak{N}$ le sont de tout ou partie, tant de* (2) *que de* (3); *le théorème a été démontré dans tous les cas où chacun de ces trois polynomes ne l'est que de tout ou partie de* (3).

Nommons $\mathfrak{Q}$ le quotient de la division du produit $\mathfrak{L}\mathfrak{M}$, par $\mathfrak{N}$, qui est supposée possible.

1° Si $\mathfrak{M}$ est déchevêtré des variables (3) encore, il se réduit à une constante, et le point en question est évident. Car le quotient $\mathfrak{Q} : \mathfrak{M}$ est un polynome entier semblable à $\mathfrak{Q}$ (3, I), et l'identité

$$\mathfrak{L}\mathfrak{M} = \mathfrak{Q}\mathfrak{N} \tag{26}$$

donne immédiatement $\mathfrak{L} = (\mathfrak{Q} : \mathfrak{M})\,\mathfrak{N}$.

2° Sinon, soient $\mathfrak{m}_1$, $\mathfrak{m}_2$, $\mathfrak{m}_3$, ..., $\mathfrak{m}_j$ des facteurs premiers en lesquels $\mathfrak{M}$ peut être décomposé (*Ib.*, III), facteurs tous déchevêtrés de (2) puisqu'il en est ainsi pour leur produit $\mathfrak{M}$ (1, VI). L'identité (26) s'écrira

$$\mathfrak{L}\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3\ldots\mathfrak{m}_j = \mathfrak{Q}\mathfrak{N}, \tag{27}$$

et, comme $\mathfrak{m}_1$ divise le premier membre (3, V), il divisera le second, mais non le facteur premier $\mathfrak{N}$ de

celui-ci; car il lui serait semblable (*Ib.*, II), et, divisant $\mathfrak{m}_1$, $\mathfrak{N}$ diviserait $\mathfrak{M}$ (*Ib.*, V) contrairement à l'hypothèse. Ce facteur $\mathfrak{m}_1$ divise donc $\mathfrak{Q}$ (I), et, en nommant $\mathfrak{Q}_1$ le quotient $\mathfrak{Q} : \mathfrak{m}_1$ de cette division, celle des deux membres de (27) par le même diviseur conduit à

$$\mathfrak{L}\,\mathfrak{m}_2\mathfrak{m}_3\ldots\mathfrak{m}_j = \mathfrak{Q}_1\mathfrak{N} \quad (3, \mathrm{V}).$$

On prouvera de la même manière que $\mathfrak{m}_2$ divise $\mathfrak{Q}_1$, puis que $\mathfrak{m}_3, \ldots, \mathfrak{m}_j$ divisent $\mathfrak{Q}_2, \ldots, \mathfrak{Q}_{j-1}$ quotients de ces divisions enchaînées. En nommant enfin $\mathfrak{Q}_j$ celui de la dernière, on obtiendra successivement les identités

$$\mathfrak{L}\,\mathfrak{m}_3\ldots\mathfrak{m}_j = \mathfrak{Q}_2\mathfrak{N}, \quad \ldots, \quad \mathfrak{L}\,\mathfrak{m}_j = \mathfrak{Q}_{j-1}\mathfrak{N}, \quad \mathfrak{L} = \mathfrak{Q}_j\mathfrak{N},$$

dont la dernière formule précisément le fait à établir.

III. *$\mathfrak{L}$, $\mathfrak{M}$, $\mathfrak{N}$ sont enchevêtrés chacun, de tout ou partie du groupe* (3) *et de x seulement dans l'autre* (2), *ceci à des degrés quelconques* ℓ, $\mathfrak{m}$, $\mathfrak{n}$; *le théorème a été démontré dans tous les cas où chacun des trois polynomes ne l'est que de tout ou partie de* (3).

Entre $\mathfrak{M}$, $\mathfrak{N}$ nous éliminerons x par la relation

$$(28) \qquad \mathfrak{P}\mathfrak{M} + \mathfrak{Q}\mathfrak{N} = {}^{(x)}\mathfrak{F},$$

où ${}^{(x)}\mathfrak{F}$ est déchevêtré de x, où les degrés (en x) de $\mathfrak{P}$, $\mathfrak{Q}$ sont $\mathfrak{p} < \mathfrak{n}$, $\mathfrak{q} < \mathfrak{m}$ (5).

1° *Sous les hypothèses actuelles* (III), *et si notre théorème est vrai pour* $\mathfrak{n} = \nu$, *entier* $\geqq 1$, *il l'est encore pour* $\mathfrak{n} = \nu + 1$.

Supposons $\mathfrak{n} = \nu + 1$.

A. *Tout polynome premier* $\mathfrak{p}$ *dont le degré* (*en x*) *est* $\leqq \nu$, *et qui divise le produit* $\mathfrak{Q}\mathfrak{N}$, *divise* $\mathfrak{Q}$ *aussi.*

Dissemblable au polynome premier $\mathfrak{N}$, comme étant de degré inférieur à $\nu + 1$ degré de celui-ci, il ne peut le diviser.

Si $\mathfrak{p}$ est déchevêtré de x, il divise $\mathfrak{Q}$ par application du dispositif de l'alinéa I.

S'il en est enchevêtré, $\mathfrak{Q}$ l'est forcément aussi. Autrement $\mathfrak{Q}$ serait non divisible par $\mathfrak{p}$, le dispositif de l'alinéa II serait applicable aux trois polynomes $\mathfrak{N}$, $\mathfrak{Q}$, $\mathfrak{p}$ (substitués respectivement à $\mathfrak{L}$, $\mathfrak{M}$, $\mathfrak{N}$ du lieu cité), et $\mathfrak{N}$ serait divisible par $\mathfrak{p}$ contrairement à ce que nous venons de constater. Les polynomes $\mathfrak{Q}$, $\mathfrak{N}$, $\mathfrak{p}$ sont alors enchevêtrés de x, tous trois; le troisième est premier, de degré $< \nu + 1$, et divise $\mathfrak{Q}\mathfrak{N}$ sans diviser $\mathfrak{N}$; il divise donc $\mathfrak{Q}$ en vertu de l'hypothèse additionnelle propre au présent sous-alinéa 1°.

B. *Le polynome* ${}^{(x)}\mathfrak{F}$ *est non-nul.*

Autrement la relation (28) donnerait

$$\mathfrak{P}\mathfrak{M} = -\mathfrak{Q}\mathfrak{N},$$

ce dont nous allons reconnaître l'impossibilité.

Si $\mathfrak{P}$ se réduit à une constante, $-\mathfrak{Q} : \mathfrak{P}$ serait un polynome entier, et l'on aurait $\mathfrak{M} = (-\mathfrak{Q} : \mathfrak{P})\mathfrak{N}$, chose impossible puisque nous admettons que $\mathfrak{M}$ n'est pas divisible par $\mathfrak{N}$.

Sinon, tout facteur premier de $\mathfrak{P}$ diviserait $\mathfrak{Q}\mathfrak{N}$, $\mathfrak{Q}$ par suite (A), parce que son degré, égal au plus à celui de $\mathfrak{P}$ qui est essentiellement inférieur à $\nu + 1$ degré de $\mathfrak{N}$, est $\leqq \nu$. En raisonnant ensuite comme tout à l'heure (II, 2°), on trouverait que $\mathfrak{M}$ est divisible par $\mathfrak{N}$, contrairement à ce que nous avons supposé.

C. Finalement, si l'on multiplie (28) par $\mathfrak{L}$, il vient

$$(29) \qquad \mathfrak{P}(\mathfrak{L}\mathfrak{M}) + \mathfrak{Q}\mathfrak{L}(\mathfrak{N}) = \mathfrak{L}\,{}^{(x)}\mathfrak{F},$$

ceci montrant que $\mathfrak{N}$ divise $\mathfrak{L}^{(x)}\mathfrak{F}$, comme divisant $\mathfrak{L}\mathfrak{M}$ par hypothèse, $\mathfrak{N}$ en fait, les deux parties du premier membre par suite (3, IV). Or, enchevêtré de x, il ne peut diviser le second facteur ${}^{(x)}\mathfrak{F}$ de ce produit, qui, non-nul (B), en est au contraire déchevêtré. Il en divise donc l'autre facteur $\mathfrak{L}$ (II).

2° *Sous les mêmes hypothèses* (III), *notre théorème est vrai pour* $\mu = 1$.

Les raisonnements sont identiques à ceux des sections (A), (B), (C) du sous-alinéa précédent (1°), avec cette simplification pourtant que, $\rho < \mu$ étant ici $= 0$, tous les facteurs premiers de $\mathfrak{P}$ sont, comme lui-même, déchevêtrés de x.

3° *Sous les mêmes hypothèses* (III), *notre théorème est vrai pour toutes les valeurs de* μ. Conséquence immédiate de la combinaison des sous-alinéas 1°, 2°.

IV. $\mathfrak{L}$, $\mathfrak{M}$, $\mathfrak{N}$ *sont enchevêtrés de* x, *déchevêtrés de toutes autres variables; rien du théorème n'a encore été établi.*

Les raisonnements sont ceux de l'alinéa III, avec les menues modifications suivantes :

Dans la section A de son sous-alinéa 1°, $\mathfrak{p}$ ne peut être déchevêtré de x, puisque, ne dépendant alors d'aucune variable, il se réduirait à une constante et ne serait pas un *diviseur* du produit $\mathfrak{P}\mathfrak{N}$ (3, II); si $\mathfrak{P}$ n'était pas enchevêtré de x, il se réduirait à une constante pour la même cause, et, semblable alors au polynome premier $\mathfrak{N}$, le produit en question ne pourrait être divisible par $\mathfrak{p}$, contrairement à l'hypothèse spéciale à cette section.

Dans la section B du même sous-alinéa, le polynome

non nul ${}^{(x)}\mathcal{F}$ se réduit à une constante Φ, puisque, déchevêtré essentiellement de x, la seule variable de la question, il ne dépend d'aucune.

Dans le sous-alinéa 2°, $\mathfrak{P}$ se réduit à une constante Π, et la relation finale (29) prend la forme

$$\Pi(\mathfrak{L}\mathfrak{M}) + \mathfrak{Q}\mathfrak{L}(\mathfrak{N}) = \mathfrak{L}\Phi,$$

sur laquelle la divisibilité de $\mathfrak{L}$ par $\mathfrak{N}$ est plus visible encore.

V. Des cas examinés ci-dessus, on passe à tous les autres par la marche progressive dont les premières et principales étapes sont indiquées ci-après, avec leurs références.

α. — *$\mathfrak{N}$, $\mathfrak{M}$, $\mathfrak{L}$ sont enchevêtrés de x seulement* [(IV)].

β. — *$\mathfrak{N}$ est enchevêtré de x seulement; $\mathfrak{M}$, $\mathfrak{L}$ le sont de x, y seulement* [(α), (I)].

γ. — *$\mathfrak{N}$ est enchevêtré de x, y seulement; $\mathfrak{M}$ ne l'est que de y; $\mathfrak{L}$ est comme $\mathfrak{N}$* [(α), (β), (II)].

δ. — *$\mathfrak{N}$, $\mathfrak{M}$, $\mathfrak{L}$ sont enchevêtrés de x, y seulement* [(α), (β), (γ), (III)].

ε. — *$\mathfrak{N}$ est enchevêtré de x, y seulement; $\mathfrak{M}$, $\mathfrak{L}$, de x, y, z seulement* [(α), (β), (γ), (δ), (I)].

η. — *$\mathfrak{N}$ est enchevêtré de x, y, z; $\mathfrak{M}$ ne l'est que de y, z; $\mathfrak{L}$ est comme $\mathfrak{N}$* [(α), (β), (γ), (δ), (ε), (II)].

. . . . . .

(La condition imposée à $\mathfrak{N}$, $\mathfrak{M}$, $\mathfrak{L}$ de dépendre des variables successivement désignées, par voie d'enchevêtrement *proprement dit,* non à titre simplement *nominal,* a eu pour but de donner brièveté et complète précision à la spécification de ces divers cas, et

d'en montrer plus nettement la progression. Mais, dans le cas (β) par exemple, l'un des polynomes $\mathfrak{M}$, $\mathfrak{L}$ pourrait être déchevêtré de y, tous deux pourraient être enchevêtrés d'autres variables quelconques accompagnant x. Et de même dans les autres.)

7. *Un polynome premier* $\mathfrak{N}$ *qui divise le produit* $\mathfrak{M}_1 \mathfrak{M}_2 \ldots \mathfrak{M}_k$ *de polynomes quelconques, divise l'un au moins d'entre eux, lui est semblable en conséquence si ce facteur est premier aussi.*

Car $\mathfrak{N}$ divise le produit de deux facteurs seulement $\mathfrak{M}_1 (\mathfrak{M}_2 \ldots \mathfrak{M}_k) = \mathfrak{M}_1 \ldots \mathfrak{M}_k$; si donc il ne divise pas $\mathfrak{M}_1$, il divisera le produit $\mathfrak{M}_2 \ldots \mathfrak{M}_k$ (6). On verra de même que, s'il ne divise pas $\mathfrak{M}_2$, il divise $\mathfrak{M}_3 \ldots \mathfrak{M}_k$, et ainsi de suite, puis finalement que, s'il ne divise pas $\mathfrak{M}_{k-1}$, il divise $\mathfrak{M}_k$.

8. *En décomposant un même polynome quelconque en facteurs premiers* (3, III), *on ne trouve jamais ceux-ci qu'en un même nombre et respectivement semblables, pour chaque décomposition, à ceux provenant de toute autre* (*conçus dans un ordre convenable*).

I. *Quand un produit* ${}_i\mathfrak{P}$ *de i polynomes premiers* $\mathfrak{N}_1, \ldots, \mathfrak{N}_i$ *est semblable à un autre produit* ${}^{(j)}\mathfrak{P}$ *de* $j \geqq i$ *facteurs de ce genre, on a* $i = j$, *et les facteurs de chacun sont respectivement semblables à ceux de l'autre* (*conçus dans un ordre convenable*).

Le facteur $\mathfrak{N}_1$ de ${}_i\mathfrak{P}$ divise évidemment le polynome semblable ${}^{(j)}\mathfrak{P}$, divise en conséquence l'un $\mathfrak{N}'$ des facteurs de celui-ci (7), lui est même semblable puisque $\mathfrak{N}_1$, $\mathfrak{N}'$ sont premiers (3, II), et les quotients

${}_i\mathfrak{P} : \mathfrak{N}_1 = \mathfrak{N}_2 \ldots \mathfrak{N}_i$, ${}^{(j)}\mathfrak{P} : \mathfrak{N}' = (\ldots)'$ sont évidemment semblables aussi.

De là on conclut, de la même manière, que $\mathfrak{N}_2$, facteur de $\mathfrak{N}_2 \ldots \mathfrak{N}_i$ est semblable à quelque facteur $\mathfrak{N}''$ de $(\ldots)'$, que les quotients ${}_i\mathfrak{P} : (\mathfrak{N}_1 \mathfrak{N}_2)$, ${}^{(j)}\mathfrak{P} : (\mathfrak{N}' \mathfrak{N}'')$ le sont encore, et ainsi de suite, jusqu'à épuisement des facteurs de ${}_i\mathfrak{P}$. A ce moment, le polynome ${}_i\mathfrak{P} : (\mathfrak{N}_1 \mathfrak{N}_2 \ldots \mathfrak{N}_i)$, auquel ${}^{(j)}\mathfrak{P} : (\mathfrak{N}' \mathfrak{N}'' \ldots \mathfrak{N}^{(i)})$ est encore semblable, se réduit à une constante; il faut donc que ce dernier se réduise aussi à une constante, ceci entraînant $i = j$.

II. De là notre théorème, puisque deux décompositions quelconques conduisent à des groupes de facteurs dont les produits sont égaux, au polynome proposé chacun, mutuellement par suite, semblables en particulier.

9. Comme on amène immédiatement des polynomes semblables à l'égalité, en les multipliant par des constantes convenables, *on peut sous-entendre l'introduction préalable de tels multiplicateurs, et, par cette convention, simplifier considérablement le langage.* Au lieu de l'énoncé précédent (8), on dira par exemple :

Tout polynome peut, d'une seule manière, être mis sous forme d'un produit de puissances de polynomes premiers inégaux (c'est à-dire dissemblables).

Le seul mot *décomposition* est très commode pour désigner cette opération et aussi son résultat.

10. Une certaine suite de théorèmes intéressants

découlent presque immédiatement de ceux des n°s 6 et 7, qui sont fondamentaux; mais, dans leurs énoncés, dans leurs démonstrations, ils ont une telle analogie avec ceux qui, en Arithmétique, se groupent autour de la décomposition des nombres entiers en facteurs premiers, qu'il serait tout à fait superflu de les exposer ici. J'en mentionnerai trois seulement, le premier appuyant tous les autres, le second et le troisième plus particulièrement utiles.

I. *La décomposition* (9) *du produit de plusieurs polynomes est le produit des facteurs inégaux qui appartiennent à l'ensemble des décompositions de ceux-ci, chacun de ces facteurs premiers étant pourvu d'un exposant égal à la somme de ceux qu'il porte dans ces diverses décompositions.*

II. *Un polynome* (*quelconque*) *qui divise un produit de deux facteurs en étant premier à l'un de ceux-ci* (3, IV) *divise l'autre* (*Cf.* 6).

III. *Quand un polynome est divisible séparément par d'autres dont deux quelconques sont premiers entre eux* (3, IV), *il l'est aussi par leur produit.*

11. Des polynomes quelconques

$$(30). \qquad \mathcal{A},\ \mathcal{B},\ \ldots,\ \mathcal{E},\ \mathcal{F},\ \ldots,\ \mathcal{H}$$

étant donnés, si, dans l'ensemble des facteurs premiers de leurs décompositions, on affecte chacun de ceux-ci du moindre des exposants qu'il porte chez les unes et chez les autres (o quand il ne figure pas dans toutes), la multiplication de ces puissances donne un nouveau polynome unique Δ, dont les propriétés caractéristiques sont maintenant très visibles.

I. *Tout diviseur de* Δ (*lui-même compris*) *est diviseur commun pour tous les polynomes proposés. Inversement, ceux-ci n'ont pas d'autres diviseurs communs que ceux de* Δ.

Ce dernier Δ est ainsi celui des diviseurs communs des proposés, dont le degré (total) est le plus grand, raison pour laquelle on le nomme *leur plus grand commun diviseur*.

[Des polynomes premiers entre eux (3, IV) n'ont pas de plus grand commun diviseur proprement dit, puisqu'ils ne sont divisibles simultanément que par des constantes (*Ib.*, II). Mais on leur attribue conventionnellement parfois une constante pour plus grand commun diviseur.]

II. *Les quotients*

$$\frac{\mathcal{A}}{\Delta}, \quad \frac{\mathcal{B}}{\Delta}, \quad \ldots, \quad \frac{\mathcal{K}}{\Delta}$$

sont premiers entre eux. Réciproquement, un polynome Δ *est le plus grand commun diviseur des proposés* (30), *s'il les divise tous, en donnant des quotients premiers entre eux.*

III. *Si le groupe* (30) *est partagé d'une manière quelconque en plusieurs sous-groupes*

$$(31) \qquad (\mathcal{A}, \mathcal{B}, \ldots), \quad (\mathcal{E}, \mathcal{F}, \ldots), \quad \ldots$$

ayant respectivement $\Delta_1, \Delta_2, \ldots$ *pour plus grands communs diviseurs, celui du groupe total est le plus grand commun diviseur de* $\Delta_1, \Delta_2, \ldots$.

Cette observation réduit la recherche du plus grand commun diviseur de polynomes en nombre quelconque, à de simples réitérations de celle concernant deux polynomes seulement.

12. En plaçant chaque facteur des décompositions des mêmes polynomes (30) sous un exposant égal au plus grand de ceux qu'il porte dans les unes et dans les autres, puis en faisant le produit de ces puissances, on forme un autre polynome ∇, unique encore, qui est caractérisé par des propriétés inverses, en quelque sorte, de celles du plus grand commun diviseur.

I. *Tout multiple de* ∇ (*lui-même compris*) *est un multiple commun de tous les polynomes* (30), (3, V). *Inversement, ceux-ci n'ont pas d'autres multiples communs que les multiples de* ∇.

Ce polynome est donc celui de moindre degré (total) parmi les multiples communs des proposés; à cause de cela, on le nomme *leur plus petit commun multiple.*

[Quand les polynomes (30) sont premiers entre eux *deux à deux,* leur plus petit commun multiple est leur simple produit (10, III).]

II. *Les quotients*

$$\frac{\nabla}{\mathfrak{A}}, \quad \frac{\nabla}{\mathfrak{B}}, \quad \ldots, \quad \frac{\nabla}{\mathfrak{K}}$$

sont premiers entre eux, et, si ∇ *est un polynome rendant de tels quotients premiers entre eux, il est le plus petit commun multiple des proposés* (*Cf.* 11, II).

III. *On peut obtenir encore le plus petit commun multiple des polynomes* (30) *en prenant celui de* ∇_1, ∇_2, ..., *polynomes remplissant la même fonction pour les sous-groupes* (31) *respectivement* (*Cf. Ib.,* III).

13. *Le plus grand commun diviseur* Γ *et le plus*

petit commun multiple Π *de deux polynomes* A, B *seulement, sont liés entre eux et à ceux-ci par la relation*

$$\Gamma\Pi = AB.$$

En nommant A′, B′ les quotients des divisions de A, B par leur plus grand commun diviseur Γ, on a $A'B'\Gamma = \Pi$, puisque $A'B'\Gamma : A = A'B'\Gamma : A'\Gamma = B'$ et $A'B'\Gamma : B = A'$ sont premiers entre eux (11, II), (12, II). Et, multipliée par Γ, cette relation donne bien $\Gamma\Pi = A'B'\Gamma^2 = A'\Gamma . B'\Gamma = AB$.

Combinée avec les observations des n°s 11 (III) et 12 (III), cette proposition ramène la recherche du plus petit commun multiple des polynomes (30) à celle des plus grands communs diviseurs d'une succession d'autres groupes se rattachant au proposé par un enchaînement que sa simplicité rend très visible.

14. La recherche du plus grand commun diviseur de polynomes donnés, celle aussi de leur plus petit commun multiple (13), ne seraient que des jeux, si la décomposition d'un polynome en facteurs premiers n'était une opération des plus ardues, dès qu'il dépend de plus d'une variable et que son degré surpasse 2. Mais ici il y a surabondance dans les conditions du problème, et, ainsi qu'il arrive en pareil cas, cette circonstance le rend impossible ou bien lui donne des facilités spéciales. La solution dérive du théorème suivant, ou bien encore de celui du n° 17 (*inf.*), dont l'application pratique semble moins laborieuse.

Pour des polynomes $\mathfrak{M}$, $\mathfrak{N}$ *tous deux enchevêtrés de* x *et sans diviseur commun déchevêtré de cette variable, soit*

$$(32) \qquad \mathfrak{P}\mathfrak{M} + \mathfrak{Q}\mathfrak{N} = {}^{(x)}\mathfrak{F}$$

la relation opérant entre eux l'élimination de x (5).

I. *Si* ${}^{(x)}\mathfrak{F}$ *est non-nul,* $\mathfrak{M}$, $\mathfrak{N}$ *sont premiers entre eux.*

II. *Si* ${}^{(x)}\mathfrak{F} = 0$, *le plus grand commun diviseur* $\mathfrak{d}$ *de* $\mathfrak{P}$, $\mathfrak{Q}$ *est déchevêtré de* x, *les quotients* $\mathfrak{P}' = \mathfrak{P} : \mathfrak{d}$, $\mathfrak{Q}' = \mathfrak{Q} : \mathfrak{d}$ *divisent* $\mathfrak{M}$, $\mathfrak{N}$ *respectivement, en donnant*

$$\frac{\mathfrak{M}}{\mathfrak{Q}'} = \frac{-\mathfrak{N}}{\mathfrak{P}'}, \tag{33}$$

et chacun de ces polynomes égaux est le plus grand commun diviseur des proposés.

I. Si $\mathfrak{M}$, $\mathfrak{N}$ avaient un diviseur commun, celui-ci serait enchevêtré de x, puisqu'ils n'en ont aucun qui en soit déchevêtré. Appartenant au premier membre de (32), ce diviseur en diviserait le second ${}^{(x)}\mathfrak{F}$ aussi. Or c'est impossible, puisqu'il est enchevêtré de x, alors que ${}^{(x)}\mathfrak{F}$, non-nul, en est essentiellement déchevêtré.

II. 1° *Dans aucune des relations* (15), *les multiplicateurs* P_i, Q_i *n'ont un diviseur premier commun qui soit enchevêtré de* x.

Si un tel diviseur existait, il diviserait ${}^{(x)}\mathfrak{p}_i Q_{i+1}$ d'après la première formule de la paire (17), Q_{i+1} deuxième facteur de ce produit par suite, puisqu'il n'en divise pas le premier ${}^{(x)}\mathfrak{p}_i$ essentiellement déchevêtré de x (6). Divisant ainsi Q_i et Q_{i+1} à la fois, il diviserait P_{i+1} aussi en vertu de la seconde formule de la même paire. Divisant simultanément P_{i+1}, Q_{i+1}, on trouverait semblablement qu'il divise P_{i+2}, Q_{i+2}, puis P_{i+3}, Q_{i+3}, puis ..., jusqu'à P_{j+1}, Q_{j+1}. Or ce dernier fait est impossible, puisque P_{j+1} est donné par la

première des formules (16), dont le second membre est essentiellement déchevêtré de x.

2° En particulier, P, Q, dans la première de ces relations, jouissent de cette propriété, $\mathfrak{P}$, $\mathfrak{Q}$ aussi, pris égaux à ces polynomes (18). Le plus grand commun diviseur $\mathfrak{D}$ de ces derniers est donc déchevêtré de x (11).

3° L'hypothèse ${}^{(x)}\mathfrak{F} = 0$ et la division simultanée de $\mathfrak{P}$, $\mathfrak{Q}$ par $\mathfrak{D}$ réduisent la relation (32) à

$$\mathfrak{P}'\mathfrak{M} = -\mathfrak{Q}'\mathfrak{N}, \tag{34}$$

celle-ci montrant que $\mathfrak{P}'$ divise le produit $\mathfrak{Q}'\mathfrak{N}$. Mais $\mathfrak{P}' = \mathfrak{P} : \mathfrak{D}$ est premier à $\mathfrak{Q}' = \mathfrak{Q} : \mathfrak{D}$ (11, II); il divise donc $\mathfrak{N}$ (10, II). Pour une cause semblable, $\mathfrak{Q}'$ divise $\mathfrak{M}$, et (34) conduit à (33).

4° Les quotients

$$\mathfrak{M} : (\mathfrak{M} : \mathfrak{Q}') = \mathfrak{Q}', \qquad \mathfrak{N} : (-\mathfrak{N} : \mathfrak{P}') = -\mathfrak{P}'$$

étant premiers entre eux, comme nous venons de le dire, chacun des deux membres de (33) est bien le plus grand commun diviseur de $\mathfrak{M}$, $\mathfrak{N}$ (11, II).

15. Maintenant, et en supposant remplies les conditions voulues pour l'existence du plus grand commun diviseur, on peut amorcer comme il suit la gradation qui conduit à celui de deux polynomes quelconques $\mathfrak{M}$, $\mathfrak{N}$.

α. — *$\mathfrak{M}$, $\mathfrak{N}$ sont enchevêtrés d'une seule variable x.*

Comme ils ne peuvent avoir aucun diviseur commun déchevêtré de x, le théorème (14) leur est immédiatement applicable. Pour cause semblable, $\mathfrak{P}$, $\mathfrak{Q}$ sont

premiers entre eux, et $\mathfrak{M} : \mathfrak{Q} = - \mathfrak{N} : \mathfrak{P}$ est le plus grand commun diviseur cherché.

β. — $\mathfrak{M}$, $\mathfrak{N}$ *sont enchevêtrés de deux variables* x, y *seulement.*

Soient $\ldots + M_y^{(i)} x^i + \ldots$ et $\ldots + N_y^{(j)} x^j + \ldots$ leurs ordinations par rapport à x, et ∂_y le plus grand commun diviseur de tous les coefficients $\ldots$, $M_y^{(i)}$, $\ldots$, $\ldots$, $N_y^{(j)}$, $\ldots$, enchevêtré comme ceux-ci de y exclusivement (11, III), (α). Les quotients $\mathfrak{M} : \partial_y$, $\mathfrak{N} : \partial_y$ n'ont visiblement aucun diviseur commun déchevêtré de x; on formera donc leurs polynomes connexes $\mathfrak{P}_y$, $\mathfrak{Q}_y$ puis $\mathfrak{P}'_y$, $\mathfrak{Q}'_y$, ensuite leur plus grand commun diviseur $(\mathfrak{M} : \partial_y) : \mathfrak{Q}'_y = - (\mathfrak{N} : \partial_y) : \mathfrak{P}'_y$ (14, II) donnant visiblement $\mathfrak{M} : \mathfrak{Q}'_y = - \mathfrak{N} : \mathfrak{P}'_y$ pour celui de $\mathfrak{M}$, $\mathfrak{N}$.

γ. — $\mathfrak{M}$, $\mathfrak{N}$ *sont enchevêtrés de trois variables* x, y, z *seulement.*

En nommant $\partial_{y,z}$ le plus grand commun diviseur de $\ldots$, $M_{y,z}^{(i)}$, $\ldots$, $\ldots$, $N_{y,z}^{(j)}$, $\ldots$, coefficients des ordinations de $\mathfrak{M}$, $\mathfrak{N}$ par rapport à x (11, III), (β), puis $\mathfrak{P}_{y,z}$, $\mathfrak{Q}_{y,z}$ et $\mathfrak{P}'_{y,z}$, $\mathfrak{Q}'_{y,z}$, polynomes connexes à $\mathfrak{M} : \partial_{y,z}$, $\mathfrak{N} : \partial_{y,z}$ (14, II), on aura

$$(\mathfrak{M} : \partial_{y,z}) : \mathfrak{Q}'_{y,z} = - (\mathfrak{N} : \partial_{y,z}) : \mathfrak{P}'_{y,z}$$

pour le plus grand commun diviseur de ces quotients et $\mathfrak{M} : \mathfrak{Q}'_{y,z} = - \mathfrak{N} : \mathfrak{P}'_{y,z}$ pour celui de $\mathfrak{M}$, $\mathfrak{N}$.

δ. — $\mathfrak{M}$, $\mathfrak{N}$ *sont enchevêtrés de quatre variables seulement.*

Semblablement.... Et ainsi de suite.

16. Avant de poursuivre, nous avons un complément à donner au théorème du n° 4.

Dans toute quasi-division, on peut, d'une seule manière, prendre les préparateurs des quasi-divisions partielles respectivement premiers aux quasi-quotients correspondants, et l'on confère ainsi la même propriété relative à ceux, ${}^{(x)}\mathfrak{P}$, $\mathfrak{Q}$, *de toute l'opération.*

I. De même qu'au lieu cité, nous représenterons par N_u, $M_{m_i}^{(i)}$ les coefficients de x^u, x^{m_i} dans le quasi-diviseur $\mathfrak{N}$ et le quasi-dividende $\mathfrak{M}^{(i)}$ de l'opération partielle exprimée par la récurrence courante (6), par $\gamma^{(i)}$ et ${}'N_u$, ${}'M_{m_i}^{(i)}$, en outre, le plus grand commun diviseur de ces coefficients et les quotients de leurs divisions par lui.

Pour que ${}^{(x)}\mathfrak{p}^{(i)}\gamma^{(i)}{}'M_{m_i}^{(i)}$ soit divisible par $\gamma^{(i)}{}'N_u$, il faut et il suffit que ${}^{(x)}\mathfrak{p}^{(i)}{}'M_{m_i}^{(i)}$ le soit par ${}'N_u$, puis, en conséquence, que ${}^{(x)}\mathfrak{p}^{(i)}$ le soit par ${}'N_u$, puisque ce diviseur est premier à ${}'M_{m_i}^{(i)}$ (10, II). En nommant donc $\varkappa^{(i)}$ le quotient de cette dernière division, on aura

$$ {}^{(x)}\mathfrak{p}^{(i)}\, M_{m_i}^{(i)} = \varkappa^{(i)}{}'N_u\, \gamma^{(i)}{}'M_{m_i}^{(i)}, $$

polynome dont le quotient de la division par

$$ N_u = \gamma^{(i)}{}'N_u $$

est $\varkappa^{(i)}{}'M_{m_i}^{(i)}$; et, pour que ce quotient soit premier au préparateur ${}^{(x)}\mathfrak{p}^{(i)} = \varkappa^{(i)}{}'N_u$, il faut que $\varkappa^{(i)}$ se réduise à une constante, c'est-à-dire que ${}^{(x)}\mathfrak{p}^{(i)}$ soit pris égal (semblable) à ${}'N_u$ (9), cette condition étant évidemment suffisante.

Désormais, nous supposerons que les préparateurs de toutes les quasi-divisions partielles ont été déterminés de cette manière.

II. Soient alors

$$(35) \qquad {}^{(x)}\mathfrak{P}^{(i+1)}\,\mathfrak{M}^{(i+1)} = \mathfrak{Q}^{(i+1)}\,\mathfrak{N} + \mathfrak{M}^{(j+1)}$$

le résultat des éliminations successives de $\mathfrak{M}^{(j)}$, $\mathfrak{M}^{(j-1)}$, ..., $\mathfrak{M}^{(i+3)}$, $\mathfrak{M}^{(i+2)}$ entre les récurrences (7), (8) dont les premiers membres montrent les accents j, $j-1$, ..., $i+1$, et

$${}^{(x)}\mathfrak{P}^{(i)}\,\mathfrak{M}^{(i)} = \mathfrak{Q}^{(i)}\,\mathfrak{N} + \mathfrak{M}^{(j+1)}$$

celui de l'élimination de $\mathfrak{M}^{(i+1)}$ entre cette relation (35) et la récurrence

$${}^{(x)}\mathfrak{p}^{(i)}\,\mathfrak{M}^{(i)} = \mathfrak{q}^{(i)}\,\mathfrak{N} + \mathfrak{M}^{(i+1)}$$

qui se trouve immédiatement au-dessus des précédentes.

Si ${}^{(x)}\mathfrak{P}^{(i+1)}$, $\mathfrak{Q}^{(i+1)}$ *sont premiers entre eux,* ${}^{(x)}\mathfrak{P}^{(i)}$, $\mathfrak{Q}^{(i)}$ *le sont aussi.*

On a effectivement

$${}^{(x)}\mathfrak{P}^{(i)} = {}^{(x)}\mathfrak{P}^{(i+1)}\,{}^{(x)}\mathfrak{p}^{(i)}, \qquad \mathfrak{Q}^{(i)} = {}^{(x)}\mathfrak{P}^{(i+1)}\,\mathfrak{q}^{(i)} + \mathfrak{Q}^{(i+1)},$$

moyennant quoi un diviseur premier commun ν des premiers membres diviserait ${}^{(x)}\mathfrak{P}^{(i+1)}$, sinon ${}^{(x)}\mathfrak{p}^{(i)}$ (6), et ${}^{(x)}\mathfrak{P}^{(i+1)}\mathfrak{q}^{(i)}$, $\mathfrak{Q}^{(i+1)}$ dans les deux cas, puisque ${}^{(x)}\mathfrak{P}^{(i+1)}$ est déchevêtré de x, que $\mathfrak{q}^{(i)}$ est un monome en x de degré $m_i - n > m_{i+1} - n$ degré du polynome $\mathfrak{Q}^{(i+1)}$. Dans le premier cas, ν diviserait à la fois ${}^{(x)}\mathfrak{P}^{(i+1)}$, $\mathfrak{Q}^{(i+1)}$, ce qui est contraire à l'hypothèse. Dans le second, où il diviserait ${}^{(x)}\mathfrak{p}^{(i)}$ mais non ${}^{(x)}\mathfrak{P}^{(i+1)}$, il diviserait aussi $\mathfrak{q}^{(i)}$, autre facteur du produit ${}^{(x)}\mathfrak{P}^{(i+1)}\mathfrak{q}^{(i)}$, ce qui n'a pas lieu puisque ${}^{(x)}\mathfrak{p}^{(i)}$, $\mathfrak{q}^{(i)}$ sont premiers entre eux (I *in fine*).

III. Comme les préparateurs sont respectivement premiers aux quasi-quotients dans la dernière et

l'avant-dernière des récurrences (7), (8), le raisonnement précédent (II) montrera qu'il en est de même pour ${}^{(x)}\mathfrak{P}^{(j-1)}$ relativement à $\mathfrak{Q}^{(j-1)}$, puis, de là, pour ${}^{(x)}\mathfrak{P}^{(j-2)}$, $\mathfrak{Q}^{(j-2)}$, puis ..., puis enfin pour ${}^{(x)}\mathfrak{P}$, $\mathfrak{Q}$, préparateur et quasi-quotient de la quasi-division considérée.

17. *Pour les polynomes* $\mathfrak{M}$, $\mathfrak{N}$ *du n°* 14, *toujours enchevêtrés de* x *et sans diviseur commun déchevêtré de cette variable, exécutons dans les conditions du n°* 16 *les quasi-divisions* (14) *du n°* 5.

Si $\mathfrak{N}_{j+2} \neq 0$, *ces polynomes sont premiers entre eux.*

Si $\mathfrak{N}_{j+2} = 0$, *les quotients* $\mathfrak{N}'_j$, $\mathfrak{N}'_{j+1}$ *des divisions de* $\mathfrak{N}_j$, $\mathfrak{N}_{j+1}$ *par le plus grand commun diviseur* ${}^{(x)}\partial$ *des coefficients de leurs ordinations par rapport à* x *sont respectivement divisibles par* $\mathfrak{q}_{j+1}$, ${}^{(x)}\mathfrak{p}_{j+1}$, *on a*

$$\frac{\mathfrak{N}'_j}{\mathfrak{q}_{j+1}} = \frac{-\mathfrak{N}'_{j+1}}{{}^{(x)}\mathfrak{p}_{j+1}}, \tag{36}$$

et chacun de ces polynomes égaux est le plus grand commun diviseur des proposés.

I. Tout diviseur commun de $\mathfrak{M}$, $\mathfrak{N}$ divise aussi $\mathfrak{N}_1$, $\mathfrak{N}_2$, ... $\mathfrak{N}_{j+1}$, $\mathfrak{N}_{j+2}$. Il résulte en effet : de la première des récurrences (14) qu'il divise $\mathfrak{N}_1$, de la seconde, qu'il divise $\mathfrak{N}_2$ puisqu'il divise $\mathfrak{N}$, $\mathfrak{N}_1$ simultanément, et ainsi de suite jusqu'à $\mathfrak{N}_{j+2}$.

Les polynomes $\mathfrak{M}$, $\mathfrak{N}$ sont donc premiers entre eux quand $\mathfrak{N}_{j+2} \neq 0$, puisque leurs diviseurs communs, s'ils en avaient, seraient enchevêtrés de x, alors que $\mathfrak{N}_{j+2}$ en est essentiellement déchevêtré.

II. En supposant maintenant $\mathfrak{N}_{j+2} = 0$, tout poly-

nome sans diviseur déchevêtré de x, qui divise $\mathfrak{N}_{j+1}$, $\mathfrak{N}_j$ simultanément, divise encore $\mathfrak{N}_{j-1}$, $\mathfrak{N}_{j-2}$, ..., $\mathfrak{N}_1$, $\mathfrak{N}$, $\mathfrak{M}$. Car, en vertu de l'avant-dernière des récurrences (14), il divise le produit ${}^{(x)}\mathfrak{p}_j\,\mathfrak{N}_{j-1}$, son dernier facteur $\mathfrak{N}_{j-1}$ par conséquent, puisque, sans diviseur déchevêtré de x, il ne peut en avoir aucun appartenant aussi à ${}^{(x)}\mathfrak{p}_j$. Puis de même pour $\mathfrak{N}_{j-2}$, ... jusqu'à $\mathfrak{N}$, $\mathfrak{M}$.

III. Il y a identité ainsi entre le plus grand commun diviseur de $\mathfrak{M}$, $\mathfrak{N}$ et celui de $\mathfrak{N}'_j$, $\mathfrak{N}'_{j+1}$. Car tout diviseur de $\mathfrak{M}$, $\mathfrak{N}$ divise $\mathfrak{N}_j = {}^{(x)}\partial\mathfrak{N}'_j$, $\mathfrak{N}_{j+1} = {}^{(x)}\partial\mathfrak{N}'_{j+1}$ (I), puis $\mathfrak{N}'_j$, $\mathfrak{N}'_{j+1}$, comme étant sans diviseur déchevêtré de x, sans diviseur commun par suite avec ${}^{(x)}\partial$ déchevêtré de cette variable; car tout diviseur commun de $\mathfrak{N}'_j$, $\mathfrak{N}'_{j+1}$ divise aussi $\mathfrak{N}_j$, $\mathfrak{N}_{j+1}$ sans avoir un facteur déchevêtré de x, divise par suite $\mathfrak{M}$, $\mathfrak{N}$ (II).

Comme $\mathfrak{N}_{j+2} = 0$, la division par ${}^{(x)}\partial$ de la dernière relation du groupe (14) est possible et laisse

$$ {}^{(x)}\mathfrak{p}_{j+1}\,\mathfrak{N}'_j + \mathfrak{q}_{j+1}\,\mathfrak{N}'_{j+1} = 0, $$

ceci conduisant à (36), parce que, rendus premiers entre eux (16), ${}^{(x)}\mathfrak{p}_{j+1}$, $\mathfrak{q}_{j+1}$ divisent $\mathfrak{N}'_{j+1}$, $\mathfrak{N}'_j$ respectivement. Et les membres de cette relation (36) sont bien tous deux égaux au plus grand commun diviseur de $\mathfrak{N}'_j$, $\mathfrak{N}'_{j+1}$, à celui de $\mathfrak{M}$, $\mathfrak{N}$ par suite, parce que les quotients $\mathfrak{N}'_j(\mathfrak{N}'_j : \mathfrak{q}_{j+1}) = \mathfrak{q}_{j+1}$ et $\mathfrak{N}'_j(\mathfrak{N}'_{j+1} : {}^{(x)}\mathfrak{p}_{j+1}) = {}^{(x)}\mathfrak{p}_{j+1}$ sont premiers entre eux.

Aussi bien que celui du n° 14, ce théorème peut être employé à la recherche du plus grand commun diviseur de deux polynomes quelconques, dont la marche générale a été exposée tout à l'heure (15).

18. Pour terminer, voici deux théorèmes utiles, qui,

au rebours des précédents, n'ont point de pendants en Arithmétique.

Pour qu'un polynome premier $\mathfrak{N}$ divise un polynome $\mathfrak{M}$ quelconque, il est nécessaire et suffisant que toutes les valeurs des variables qui l'annulent numériquement annulent $\mathfrak{M}$ aussi.

Le premier point est évident. Pour établir le second, nous remarquerons que ces polynomes sont forcément enchevêtrés tous deux d'une même variable au moins, que nous nommerons x et que nous éliminerons entre eux par la relation

$$(37) \qquad \mathfrak{P}\mathfrak{M} + \mathfrak{Q}\mathfrak{N} = {}^{(x)}\mathfrak{F}(y, z, \ldots),$$

${}^{(x)}\mathfrak{F}$ étant déchevêtré de x, les multiplicateurs $\mathfrak{P}$, $\mathfrak{Q}$ ayant par rapport à x des degrés respectivement inférieurs à ceux de $\mathfrak{N}$, $\mathfrak{M}$ (5). Aux variables y, z, ..., dont ${}^{(x)}\mathfrak{F}$ dépend à l'exclusion de x, nous attribuerons ensuite un système quelconque y', z', ... de valeurs particulières.

Si ces valeurs annulent la totalité des coefficients de l'ordination de $\mathfrak{N}$ par rapport à x, elles annulent $\mathfrak{N}$ forcément aussi, $\mathfrak{M}$ encore par suite et par hypothèse, et, en vertu de (37), on a numériquement

$$(38) \qquad {}^{(x)}\mathfrak{F}(y', z', \ldots) = 0.$$

Si, pour $y = y'$, $z = z'$, ..., les coefficients des termes de cette ordination, où x a des exposants > 0, ne s'évanouissent pas tous, l'équation en x

$$(39) \qquad \mathfrak{N}(x, y', z' \ldots) = 0$$

a quelque racine x', donnant ainsi $\mathfrak{N}(x', y', z', \ldots) = 0$, puis, par hypothèse, $\mathfrak{M}(x', y', z', \ldots) = 0$ et (38) encore, à cause de (37).

Si les mêmes attributions numériques annulent la totalité des coefficients qui viennent d'être spécifiés, l'équation (39) ne peut être résolue; mais on verra facilement qu'à quelqu'une des variables y, z, ..., à z pour fixer les idées, on peut attribuer leur valeur z'' infiniment voisine de z', à x une valeur correspondante x'', qui donnent $\mathfrak{N}(x'', y', z'', \ldots) = 0$, d'où $\mathfrak{M}(x'', y', z'', \ldots) = 0$ par hypothèse, puis

$$^{(x)}\mathfrak{F}(y', z'', \ldots) = 0,$$

d'après la relation (37). Si maintenant on fait tendre z'' vers z', il vient

$$\lim {}^{(x)}\mathfrak{F}(y', z'', \ldots) = 0 = {}^{(x)}\mathfrak{F}(y', z', \ldots).$$

Le polynome $^{(x)}\mathfrak{F}(y, z, \ldots)$ s'évanouit donc numériquement pour toutes les combinaisons de valeurs de ses variables, c'est-à-dire identiquement. La relation (37) se réduit donc à

$$\mathfrak{P}\mathfrak{M} + \mathfrak{Q}\mathfrak{N} = 0,$$

ceci montrant que $\mathfrak{N}$ divise le produit $\mathfrak{P}\mathfrak{M}$, $\mathfrak{M}$ par suite, puisque la supériorité de son degré en x, comparé à celui de $\mathfrak{P}$, s'oppose à ce qu'il divise ce dernier polynome (6).

19. Pendant un instant, nous nommerons *grade* d'un polynome quelconque $\mathfrak{M}$, relativement à un autre premier donné $\mathfrak{N}$, l'entier $M(\geqq 0)$ jouissant de la propriété que $\mathfrak{M}$ soit divisible par $\mathfrak{N}^M$, non par $\mathfrak{N}^{M+1}$, tel ainsi, que l'on ait $\mathfrak{M} = \mathfrak{N}^M \mathfrak{Q}$, le quotient $\mathfrak{Q}$ étant non divisible par $\mathfrak{N}$.

Si maintenant on représente par

(40) $$\mathfrak{M}, \quad \mathfrak{M}', \quad \mathfrak{M}'', \quad \ldots$$

des dérivées de $\mathfrak{M}$ par rapport aux variables dont $\mathfrak{N}$ est enchevêtré, prises respectivement au hasard dans les ordres (totaux) 0, 1, 2, ..., on a ce théorème :

Le grade M *de* $\mathfrak{M}$ *est égal à l'ordre de la première des dérivées* (40) *qui n'est pas divisible par* $\mathfrak{N}$.

Toute dérivation (première) de $\mathfrak{M}$ par rapport à ces variables diminue de 1 son grade (supposé > 0). On trouve effectivement, en prenant D pour signe de cette dérivation,

$$D\mathfrak{M} = D(\mathfrak{N}^M \mathfrak{Q}) = \mathfrak{N}^M . D\mathfrak{Q} + M\mathfrak{N}^{M-1}(D\mathfrak{N} . \mathfrak{Q}),$$

et, comme $\mathfrak{N}$ est premier, il ne divise ni $D\mathfrak{N}$ ayant un degré inférieur au sien par rapport à la variable de dérivation, ni $\mathfrak{Q}$ par hypothèse. Il en résulte que le dernier terme du second membre est divisible par $\mathfrak{N}^{M-1}$, non par $\mathfrak{N}^M$ (7), puis, qu'il en est de même pour tout ce membre ayant son autre terme divisible par $\mathfrak{N}^M$. En d'autres termes, $M - 1$ est le grade de $D\mathfrak{M}$.

La réitération de ce raisonnement montre bien facilement que les grades des dérivées (40) calculées jusqu'à l'ordre M sont

$$M, \quad M - 1, \quad M - 2, \quad \ldots,$$
$$M - (M - 1) = 1, \qquad M - M = 0,$$

comme il suffisait de le constater.

Soit directement, soit par sa combinaison avec la précédente (18), cette proposition peut rendre des services dans la décomposition d'un polynome en facteurs premiers.

(Extrait des *Nouvelles Annales de Mathématiques*, 4e série, t. VII; mai 1907.)

40186 Paris. — Impr. GAUTHIER-VILLARS, quai des Grands-Augustins, 55.

0

QA 161 M47

Méray, Hugues Charles Robert
Divisibilité des polynomes entiers a plusieurs variables

Physical & Applied Sci.

PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET

UNIVERSITY OF TORONTO LIBRARY